IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Attorney Docket No.: **CA920030040US1**

In re Application of: §
§ Confirmation No.: **7948**
YANTZI §
§ Examiner: **POLTORAK, P.**
Serial No.: **10/809,563** §
§ Art Unit: **2134**
Filed: **25 MARCH 2004** §
§
For: **PASSWORD MANAGEMENT** §

APPEAL BRIEF

MS Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Notification of Non-Compliant Appeal Brief under 37 C.F.R. § 41.37 dated October 30, 2008, please replace page 3 of the previous Brief with the current page 3.

No fee or extension of time is believed to be required; however, in the event a fee or extension of time is required, please charge that fee to the IBM Deposit Account No. **09-0447**.

REAL PARTY IN INTEREST

The present application is assigned to International Business Machines Corporation, the real party of interest.

RELATED APPEALS AND INTERFERENCES

No related appeal is presently pending.

STATUS OF THE CLAIMS

Claims 1-5 and 26-30 were finally rejected by the Examiner as noted in the Final Office Action dated August 15, 2008. Claims 6-25 were canceled.

STATUS OF AMENDMENTS

An Amendment was submitted on November 13, 2007 in reply to the Non-Final Office Action dated September 12, 2007. An Amendment was submitted on February 18, 2008 in reply to the Final Office Action dated December 18, 2007. An Amendment was submitted on June 10, 2008 in reply to the non-Final Office Action dated May 21, 2008.

SUMMARY OF THE CLAIMED SUBJECT MATTER

Claim 1 recites a method of managing passwords for a set of software resources accessible by a user. A password registry is provided for storing passwords within a workstation (page 6, lines 6-7; password registry **210** of Figure **2**). Each of the software resources is allowed to register its password in the password registry via a respective one of the front-end processes within the workstation (page 7, lines 1-3; Figure **2**). Each of the passwords is encrypted by the respective front-end process before being stored in the password registry (page 8, lines 6-8; Figure **2**). In response to an access request to one of the software resources via a corresponding one of the front-end processes, a determination is made whether or not an encrypted password associated with the requested software resource is stored in the password registry (page 9, lines 17-20; block **3** of Figure **3B**). If the encrypted password associated within the requested software resource is stored in the password registry, the encrypted password is sent from the password registry to the corresponding front-end process for decryption in order to permit the access